(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－212923

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
19/00		15/30	３４０
Ｇ０７Ｆ　7/12		Ｇ０７Ｆ　7/08	Ｂ

審査請求　未請求　請求項の数４　ＯＬ　（全８頁）

(21)出願番号　特願平10－10130

(22)出願日　平成10年(1998)１月22日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　堀井　高広
神奈川県横浜市都筑区加賀原二丁目２番株式会社日立製作所ビジネスシステム開発センタ内

(74)代理人　弁理士　小川　勝男

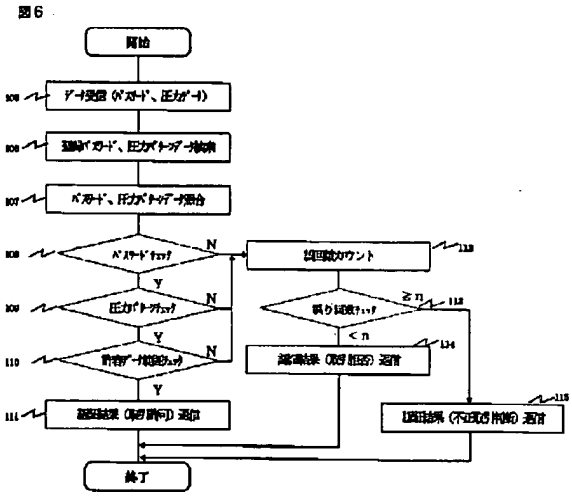
(54)【発明の名称】　金融取引における認証方法及びシステム

(57)【要約】　（修正有）

【課題】金融機関と個人、法人間の伝送路を通じた金融取引において、取引を認証するパスワードなどを第三者が不正に入手した場合に、不正取引を防ぎ、入手した第三者が保持する非接触を含むＩＣカードなどの契約情報、取引情報を不正に利用することを防ぐ。

【解決手段】本金融取引における認証方法とシステムでは、取引を行う時にパスワードを入力すると同時に圧電素子などの圧力センサーにより構成される入力鍵盤により入力時の文字に対応した圧力パターンデータを予め登録されたパターンデータと照合することにより、パスワードを不正取得した第三者の不正取引を防ぎ、又、外部から無線もしくは赤外線によりデータ消去プログラムをＩＣカードに送信し、データ消去を行うことにより上記課題を解決する。

図6



1

【特許請求の範囲】

【請求項１】金融取引要求者の文字入力部、及び文字入力部の入力鍵盤に対する圧力データ測定部と、認証システムへのデータ、プログラム送受信部、ＩＣカードインタフェースとＩＣカードによる不正取引時にＩＣカードへ送信するデータ消去プログラムの蓄積部を有する金融取引端末と専用線、オープンネットワークを通じて接続され金融取引端末から送信された入力文字データ、入力鍵盤に対する圧力データの送受信部と受信した圧力データと照合する予め登録された圧力データを元としたパターンデータ生成部、及び認証データの蓄積部を有し、圧力データを基に取引を認証する手段を有する認証システムにおいて、金融取引端末にパスワードなど取引を認証する文字が入力されると、入力文字と入力鍵盤に対する圧力データを計測し、伝送路を通じて、認証システムに入力文字データ、入力鍵盤に対する圧力データを伝送し、入力文字データ、入力鍵盤に対する圧力データを蓄積して、取引を認証する照合元入力文字パターンデータと入力鍵盤に対する入力圧力パターンデータを照合し、取引要求時に該当取引の取引認証を行う金融取引における認証方法及びシステム。

【請求項２】前記請求項１に記載の金融取引端末において、前記入力鍵盤に対する複数の圧力データからなる許容データ範囲を生成し、取引を認証する照合元入力文字パターンデータと入力鍵盤に対する圧力パターンデータを照合する手段を含むことを特徴とする金融取引における認証方法及びシステム。

【請求項３】前記請求項１に記載の金融取引端末において、前記入力鍵盤に対する圧力データを測定する手段として、圧電素子からなる圧力センサーを有することを特徴とする金融取引における認証方法及びシステム。

【請求項４】前記請求項１に記載の金融取引端末において、金融取引要求者のＩＣカードに記憶する契約情報、取引情報を消去するプログラムを記憶装置に記憶し、無線アダプタ等のデータ送受信インタフェースを有するＩＣカードなどの媒体にプログラムを送信し、ＩＣカードなどの媒体で記憶する情報を消去するプログラムを実行する金融取引における認証方法及びシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、金融機関と金融取引契約を結ぶ個人、法人などの顧客が金融取引要求時に、取引を認証するパスワード等の入力文字を入力する際の入力鍵盤に対する圧力パターンデータを利用し、特に、金融取引端末を通じた取引要求に関し、該当取引者が予め登録もしくは、過去において入力した際の圧力パターンデータ履歴を蓄積し、参照し、当該取引要求の際の入力鍵盤に対する圧力パターンデータと比較し、不正な取引を行なおうとした第三者の取引要求を拒絶し、更に、第三者が不正に入手し保有するＩＣカード媒体に記

2

憶された取引契約者の契約情報、取引情報を消去する金融機関の店頭取引、ホームバンキング、ファームバンキング、及び伝送路を通じた電子決済でのセキュリティー管理での利用に好適な金融取引における認証方法及びシステムである。

【０００２】

【従来の技術】金融機関の店頭取引、ホームバンキング、ファームバンキング、及び伝送路を通じた電子決済により金融取引を行う場合は、取引を認証する個人情報、契約情報及びキーワードを金融機関の金融取引端末もしくは、顧客の金融取引端末と公衆回線、インターネット、パソコン等のオープンな伝送路を接続行うことにより行っている。金融機関の金融取引端末及び、ネットワークを通じて金融取引を行う場合、情報システムはなりすましによる不正取引を防止する方法としてＩＤ番号、パスワード、回線認証、電子署名、本人認証などがある。

【０００３】従来の方法は、特平開５－６１８３２号公報に記載のデータ機密保護方式のように、複数の端末装置と処理装置を備えたシステムにおいて、あらかじめ利用者ごとにパスワードを利用可能な業務を示す利用権情報が登録され、利用者が業務を行う場合、端末から入力されたパスワードと利用権情報と登録された内容を比較し、業務処理要求を受け付けるか否かを判断し、受け付けると判定した場合のみ、業務処理要求に対応した処理を行う方法があった。

【０００４】従来の方法は、特平開７－８５２７６号公報に記載の個人認証方式のように、電極基盤上に儲けられた複数の線状接触子電極と電極シートと感圧シート及び対向電極とからなる指紋入力部により、指の加圧状態を抵抗値変化として捉え、接触抵抗を読みとることにより個人認証を行う方法があった。

【０００５】

【発明が解決しようとする課題】上記従来技術は、金融取引時に取引を認証するパスワードを知りうる者に対して不正取引を防げない。パスワードを本人がパスワード入力を行う際に第三者が視認によりパスワードを入手できる場合がある。もしくはなりすましを防ぐために、パスワードの定期的変更や複雑な入力手順を取引者に要求するなど取引者の容易な取引操作への配慮がされておらず、安全でかつ容易な取引ができないという問題があった。また、パスワードの強制的な強奪や、指紋や網膜情報の人体特徴照会による個人認証においては、第三者による取引者の人体への傷害を発生させえる場合があるなどの問題があった。更に、非接触のＩＣカード及びそこに含まれる契約情報、取引情報などが盗まれた場合にそれらの情報を不正取引を行おうとする第三者が保有し他に利用することを防げない。又、ＩＣカード自体にデータ消去プログラムを搭載した場合には誤動作によりデータが消去されてしまうという問題があった。

【0006】本発明の目的は、取引者の取引入力時の入力文字データと入力鍵盤に対する圧力データを関連付け、予め登録された圧力パターンデータと照合することで第三者がパスワードを入手してなすましにより不正取引を行う事を防ぐことにある。又、入力鍵盤に対する圧力パターンデータは視認では入手が難しく不正に第三者が入手できない。さらに、不正取引と判定された場合には、不正取引者の保有する契約情報、取引情報を外部からデータ消去プログラムを非接触ＩＣカードなどの媒体に送信し、ＩＣカード上のデータ処理部によりデータ消去プログラムを実行することで不正取引者の保有する情報を適切に消去せしめ、かつ外部からデータ消去プログラムをＩＣカードなどの媒体に送信することで誤動作によるデータ消去を防ぐことができる。

【0007】

【課題を解決するための手段】本発明は、上記目的を達成するために、本発明の金融取引における認証方法及びシステムは、取引を認証するパスワードを入力する際に、入力文字データを入力部により入力し、入力鍵盤と接触する指部により生じる圧力データを圧電素子からなるデータ測定部により電圧値として測定し、入力鍵盤全体に対する電圧値を認証システムに送受信部により送信し、認証システムではこの電圧値データを受信して、取引時の圧力パターンデータと予め登録された文字に対応する前記圧力パターンデータを照合する認証部を備えることを特徴とする。

【0008】又、上記目的を達成するために、本発明の金融取引における認証方法及びシステムは、ＩＣカードに蓄積される契約情報、取引情報を消去するの手段として、ＩＣカードと金融取引端末において、不正取引と判断された場合にデータ消去プログラムを、無線通信もしくは赤外線通信手段により送受信する送受信部、データ消去プログラムを蓄積する蓄積部、実行するデータ処理部を有することを特徴とする。

【0009】上記手段に基づく作用として、金融機関と取引を行う金融取引端末において、取引を複数の情報をもとに認証し、不正な取引者の保有するデータを消去するプログラムを不正取引と認証した時点でＩＣカードなどの媒体に伝送することにより、第三者が本人認証情報を不正に入手することを防止し、かつ金融取引時に第三者による不正取引を防止し、不正取引と判断される場合にはＩＣカードの情報を消去することで不正な第三者による情報の不正利用を防止することができる。

【0010】

【発明の実施の形態】以下、本発明の実施例を図面に基づいて詳細に説明する。図１は本発明の一実施例を示す金融取引における認証方法及びシステムの全体概念図であり、図２はその要部である金融取引端末のブロック構成図、図３は認証システムを構成するブロック構成図、図４はＩＣカードのブロック構成図である。

【0011】図１において、１は金融機関と取引のある個人もしくは企業が利用し、金融機関の店頭、もしくはネットワークを通じての金融取引のための契約情報、取引情報などを送受信管理し、取引者が取引認証のために入力したパスワードなどの文字データと文字入力時の圧力データを認証システムへ送信し、及び認証システムからの認証結果を受けて取引実行もしくはパスワードの再入力受付、登録された入力文字パターンデータと取引時の入力圧力パターンデータと一致しない複数回の入力の試みに対して認証システムが不正取引と判断し、金融取引端末にアラーム送信し、金融取引端末がアラームを受信すると、前記不正取引と判断され使用されるＩＣカードにデータ消去プログラムを送信する金融取引端末である。２は金融取引端末から送信されたデータを受信管理し、受信した文字データ、圧力データと予め登録されたデータを基にパターンデータを生成し、照合処理し、金融取引時の取引の認証を行い、金融取引端末に認証結果を返信する認証システムである。３は取引要求者が金融取引端末と取引データを送受信する際に使用するＩＣカードなどのデータ記憶媒体である。４は専用回線、オープンネットワークを含む伝送路である。

【0012】図２において、金融取引端末１は、制御部１１、入力部１２、表示部１３、データ処理部１４、データ蓄積部１５、データ測定部１６、送受信部１７、ＩＣカードインタフェース１８から構成される。このうち、上記全体制御装置１１は、全体制御部１１１、データ制御部１１２、通信制御部１１３から構成される。図３において、認証システム金融機関端末２は、制御部２１、認証部２２、データ処理部２３、パターンデータ生成部２４、認証データ蓄積部２５、送受信部２６、アラーム２７から構成される。このうち、上記制御部２１は、全体制御部２１１、データ制御部２１２、通信制御部２１３、データチェック部２１４から構成される。図４において、ＩＣカード３は、制御部３１、記憶部３２、データ処理部３３、送受信部３４から構成される。このうち、制御部３１は、全体制御部３１１、記憶制御装置３１２、通信制御部３１３から構成される。図５は、金融取引端末への取引要求に対して、ＩＣカードデータの契約情報を受信し、入力文字データ、文字入力圧力データを測定して認証システムに送信する処理フローである。

【0013】前記金融取引端末１は、取引要求者からの取引要求時に、ＩＣカードインタフェース１８により図１０に記載のＩＣカードに記憶する契約情報を受信し（ステップ１０１）、入力部１２により取引を認証するパスワード入力を受付ける（ステップ１０２）。この時、データ測定部１６で図９に記載の入力鍵盤及び付属する圧電素子に対して取引者の指部の文字入力圧力から電圧値データを計測し（ステップ１０３）、認証システムに図１１に記載の入力文字データ、入力圧力データを

送信する（ステップ104）。図6は、前記金融取引端末1からの取引要求及び取引要求者の契約情報、文字入力に対する圧力データを受信して予め登録されている取引要求者の契約情報に基づき取引者を認証するパスワード、圧力パターンデータを検索照合し、前記金融取引端末1に認証結果（取引許可、取引拒否、不正取引判断）を返信する処理フローである。

【0014】前記認証システム2は、金融取引端末1から送信される入力文字データと圧力パターンデータを送受信部26にて受信し（ステップ105）、まず、認証データ蓄積部25において図12に記載の予め登録されているパスワードとパターンデータ生成部24にて生成される圧力パターンデータのテーブルを検索する（ステップ106）。次に、この検索した取引者の登録されているパスワード、圧力パターンデータと取引要求時のパスワード及び圧力パターンデータを図13に記載のチェックテーブルにより照合する（ステップ107）。この時、パスワードのチェック（ステップ108）、圧力パターンチェック（ステップ109）を行い、また、過去の取引時の圧力データを元に入力鍵盤に対する圧力許容データ範囲を設定し、データの範囲チェックを行う（ステップ110）。更に、同一取引要求者からの繰り返し行われる取引要求時の入力誤りに対しては取引要求者の前記金融取引端末1に対して取引拒否の認証結果を送信し（ステップ114）、なおかつ取引回数を図14に記載の誤り回数カウントテーブルによりカウント（ステップ112）してその誤り回数が任意の設定回数を超えたかﾁｪｯｸして（ステップ113）、超えた場合には不正取引判断を前記金融取引端末に返信する（ステップ115）。図7は、前記認証システム2からの認証結果を受信し、取引実行もしくは取引拒否メッセージ、再パスワード入力指示を取引要求者に表示し、不正取引者と判断した場合にはICカードの記憶するデータを消去するプログラムを送信する処理フローである。

【0015】前記金融取引端末1は、認証システム2から図15に記載の認証結果を受信し（ステップ116）、認証結果より取引許可かどうかをﾁｪｯｸし（ステップ117）、取引許可ならば取引要求者の取引を実行し（ステップ118）、取引許可でなければ、次に認証結果より、不正取引チェック（ステップ119）を行って、認証結果が取引拒否であるならば、取引拒否メッセージを表示し（ステップ120）、再パスワード入力指示を行って（ステップ121）、さらに認証結果が不正取引判断であるならば、データ消去プログラムをICカードなどの媒体に送信する（ステップ122）。図8は、前記金融取引端末1からデータ消去プログラムを受信、記憶し、データ消去を実行するICカードでの処理フローである。

【0016】前記ICカード3は、金融取引端末からのデータ消去プログラムを送受信部34で受信し（ステップ123）、記憶部32に一時記憶し、データ処理部33にて記憶部32に記憶する契約データ、図16に記載の取引データの消去を実行する（ステップ124）。

又、データ消去プログラムを認証システムにて記憶し、金融取引端末及びICカードに送信することを含む。図9は、前記金融取引端末の入力部及び入力鍵盤と入力鍵盤の取引要求者の文字入力時の接触状態を示す例であり、121は入力鍵盤上の指部が文字入力の際に接触する部分に設置される圧電素子でさる。図17は、前記認証システム2において過去取引のデータの時系列の圧力データを基に回帰直線を設定し、回帰直線から任意に設定した上限、下限に基づいて許容データ範囲を設定する例である。

【0017】

【発明の効果】本発明によれば、金融機関に対する資金移動、入出金、決済などの金融取引を行う顧客が取引要求を金融機関に行うときにパスワードなどと前記認証方法を合わせて行うことにより、顧客のパスワードが不正に取得された場合された場合にも不正取引を防ぐことができ、不正取引を試みる第三者が保持するICカードの契約情報、取引情報を消去してこの情報の不正使用を防ぐことが期待できる。

【図面の簡単な説明】

【図1】金融取引端末、認証システム、ネットワーク及びICカードからなる本発明の金融取引の認証方法とシステムの全体概要図。

【図2】前記金融取引端末の装置構成。

【図3】前記認証システムの装置構成。

【図4】前記ICカードの装置構成。

【図5】金融取引端末への取引要求に対して、ICカードデータの契約情報を受信し、入力文字データ、文字入力圧力データを測定して認証システムに送信する処理フローである。

【図6】前記金融取引端末1からの取引要求及び取引要求者の契約情報、文字入力に対する圧力データを受信して予め登録されている取引要求者の契約情報に基づき取引者を認証するパスワード、圧力パターンデータを検索照合し、前記金融取引端末1に認証結果（取引許可、取引拒否、不正取引判断）を返信する処理フローである。

【図7】前記認証システム2からの認証結果を受信し、取引実行もしくは取引拒否メッセージ、再パスワード入力指示を取引要求者に表示し、不正取引者と判断した場合にはI.Cカードの記憶するデータを消去するプログラムを送信する処理フローである。

【図8】前記金融取引端末1からデータ消去プログラムを受信、記憶し、データ消去を実行するCカードでの処理フローである。

【図9】前記金融取引端末1の入力部及び入力鍵盤と入力鍵盤の取引要求者の文字入力時の接触状態を示す例である。

7

【図10】前記ＩＣカード３に記憶し、取引要求時に金融機関端末に送信する取引要求者が金融機関と取引を契約する契約情報の例である。

【図11】前記金融取引端末１から前記認証システム２に送信する取引要求時の入力パスワードと入力圧力データのデータの例である。

【図12】前記認証システム２において、前記金融取引端末１からの受信する取引要求データと照合する予め登録されている照合元パスワードと圧力パターンデータテーブルの例である。

【図13】前記認証システム２において、前記金融取引端末１からの受信する取引要求データと予め登録されている照合元パスワードと圧力パターンデータテーブルの照合結果テーブルの例である。

【図14】前記認証システム２において、前記金融取引端末１からの繰り返し行われる取引要求に対して入力誤り回数をカウントする不正取引判断の誤り回数カウントテーブルの例である。

【図15】前記認証システム２から、前記金融取引端末１に対して返信する認証結果のデータ例である。

【図16】前記ＩＣカード３において、前記金融取引端

8

末から受信したデータ消去プログラムにより、データ消去される取引データテーブルの例である。

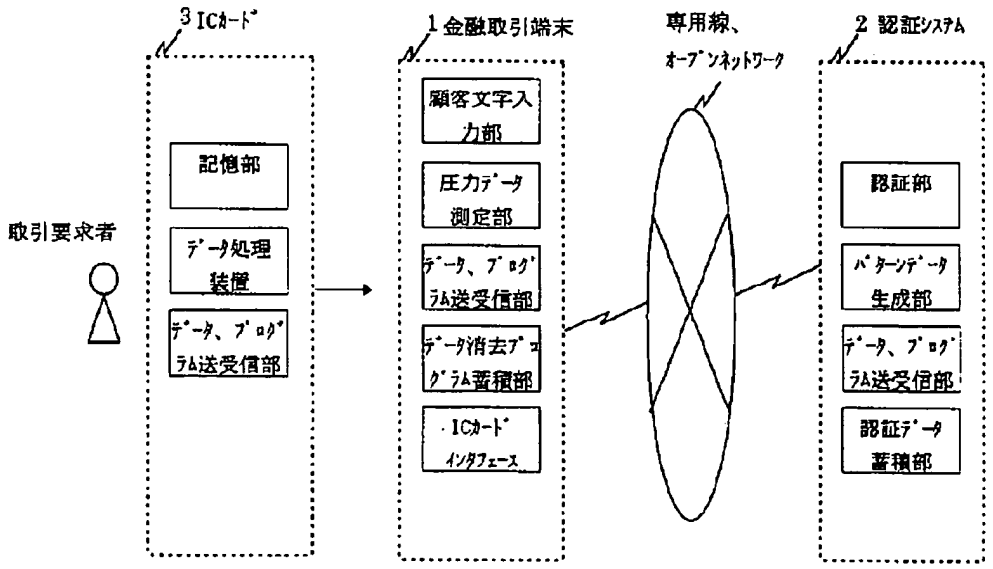
【図17】前記認証システム２において過去取引のデータの時系列の圧力データを基に回帰直線を設定し、回帰直線から任意に設定した上限、下限に基づいて許容データ範囲を設定する例である。

【符号の説明】

１…金融取引端末、　２…認証システム、　３…ＩＣカード、４…ネットワーク、　１１…制御部、１２…入力部、　１２１３…表示部、　１４…データ処理部、１５…データ蓄積部、　１６…データ測定部、１７…送受信部、１８…ＩＣカードインタフェース、　１１１…全体制御部、１１２…データ制御部、１１３…通信制御部、　２１…制御部、２２…認証部、　２３…データ処理部、２４…パターンデータ生成部、２５…認証データ蓄積部、　２６…送受信部、２７…アラーム部、　２１１…全体制御部、２１２…データ制御部、２１３…通信制御部、　２１４…データチェック部、３１…制御部、３２…記憶部、　３３…データ処理部、３４…送受信部、　３１１…全体制御部、３１２…記憶制御部、３１３…通信制御部。

【図1】

図1



【図15】

図15

送信No	認証コード
113215	1

【図10】

図10

顧客名	店番	口座番号	取引コード	パスワード	圧力データ1	圧力データ	圧力データ	圧力データ
鎌谷恵一	312	6125127	010					

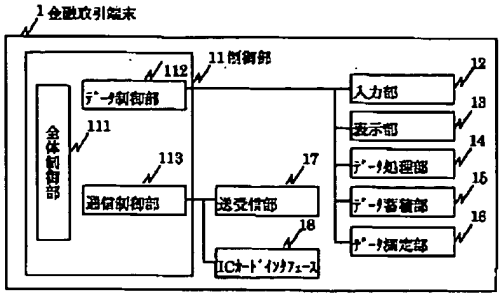
【図11】

図11

顧客名	店番	口座番号	取引コード	パスワード	圧力データ1	圧力データ2	圧力データ3	圧力データ4
鎌谷恵一	312	6125127	010	2135	35	30	30	70

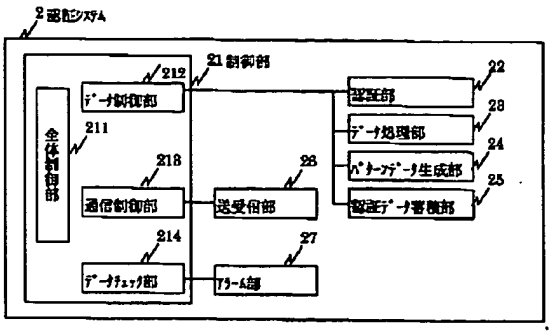
【図2】

図2



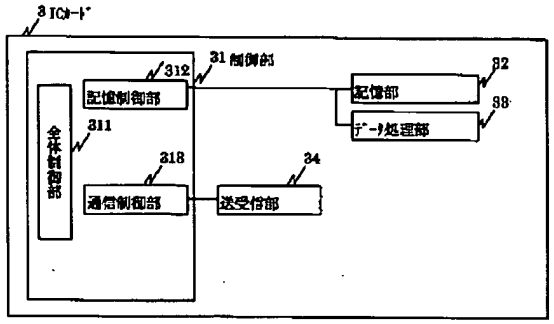
【図3】

図3



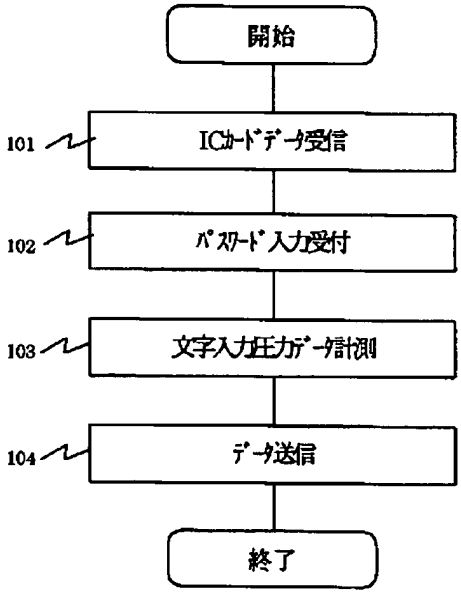
【図4】

図4



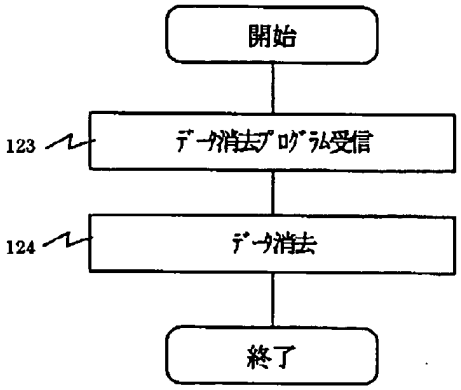
【図5】

図5



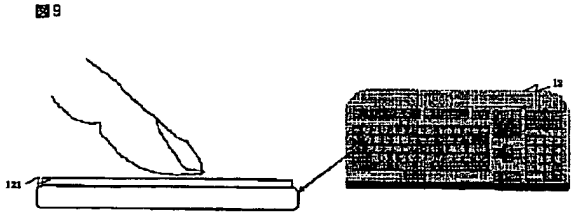
【図8】

図8



【図9】

図9



【図12】

図12

顧客名	店番	口座番号	取引コード	パスワード	圧力データ1	圧力データ2	圧力データ3	圧力データ4
鹿谷恵一	312	6125127	010	2135	x<50	x<50	x<50	50≦x≦80

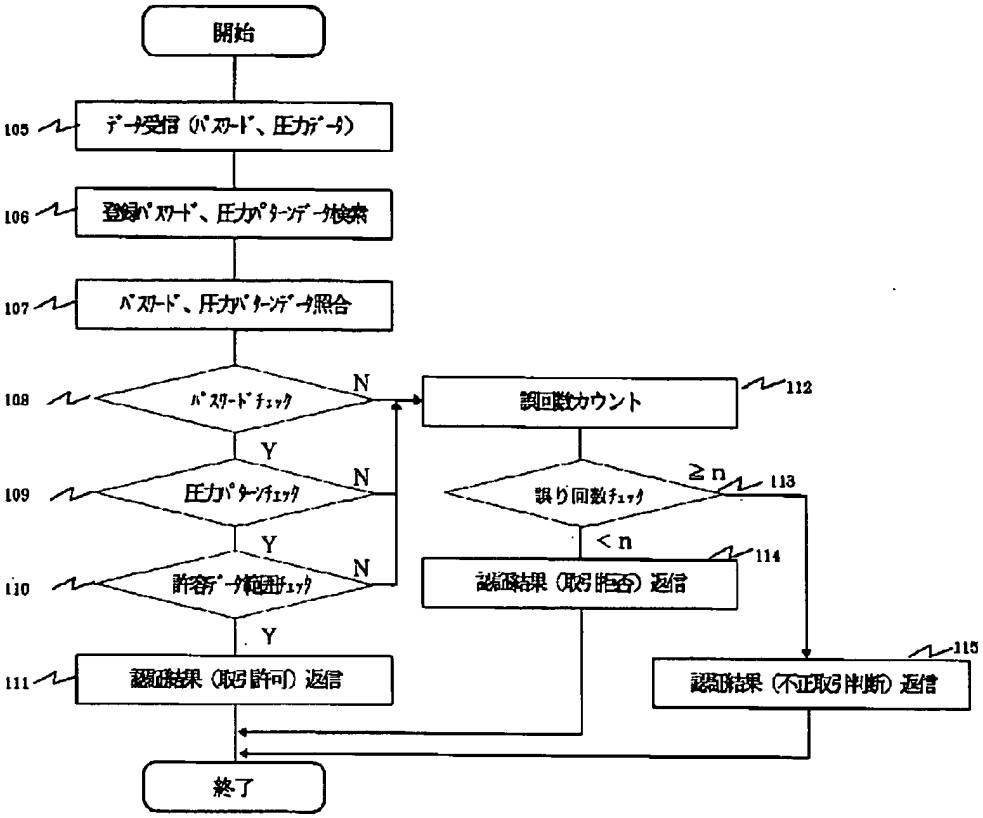
【図13】

図13

顧客名	店番	口座番号	取引コード	照合データ1	照合データ2	照合データ3	照合データ4	照合データ5
鹿谷恵一	312	6125127	010	1	1	1	1	1

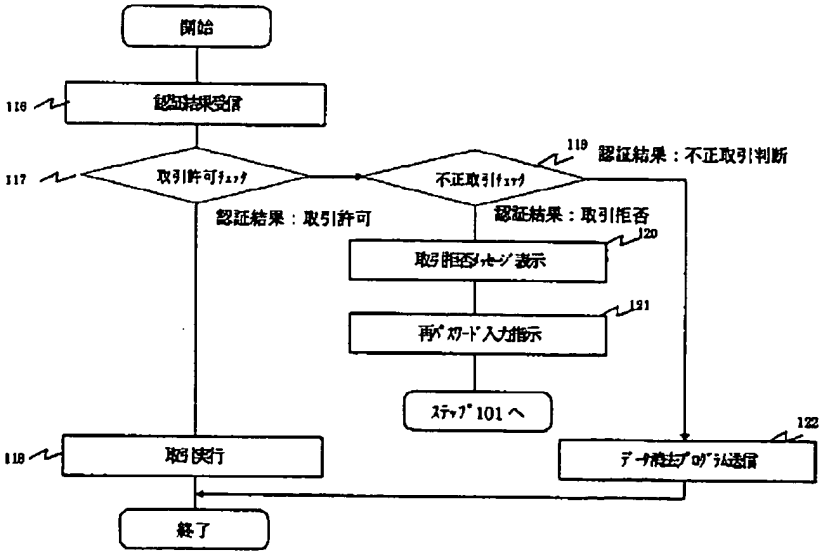
【図6】

図6



【図7】

図7



【図14】

図14

顧客名	店番	口座番号	取引コード	誤り回数
藤谷恵一	312	6125127	010	5

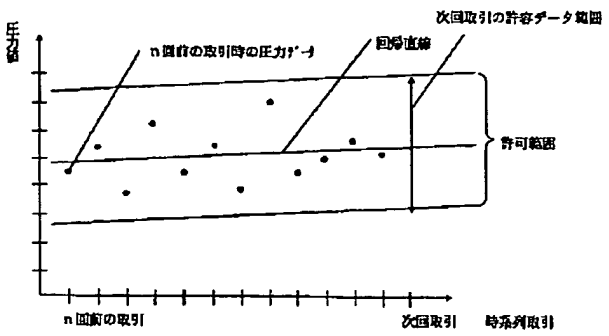
【図16】

図16

取引No	店番	取引種別	取引金額	取引日	取引時間	口座ﾃﾞｰﾀ1	口座ﾃﾞｰﾀ2
1	312	口座振替	10000	19970901	00142434	6125127	3005127
2	312	出金	3000	19970905	00152411	6125127	3005127
3	312	振込	6000	19970906	00142121	6125127	3006127

【図17】

図17



PAT-NO: JP411212923A

DOCUMENT-IDENTIFIER: JP 11212923 A

TITLE: AUTHENTICATION METHOD AND SYSTEM FOR FINANCIAL TRANSACTION

PUBN-DATE: August 6, 1999

INVENTOR-INFORMATION:
NAME COUNTRY
HORII, TAKAHIRO N/A

ASSIGNEE-INFORMATION:
NAME COUNTRY
HITACHI LTD N/A

APPL-NO: JP10010130

APPL-DATE: January 22, 1998

INT-CL (IPC): G06F015/00, G06F019/00 , G07F007/12

ABSTRACT:

PROBLEM TO BE SOLVED: To prevent a wrong financial transaction that is executed via a transmission line set between a

financial institution and a
private or juridical person when a password, etc.,
which authenticates the
transaction is wrong acquired by a third person and
also to prevent the third
person from using wrong the contract and
transaction information on the IC
cards including the contactless one, etc., of the
third person.

SOLUTION: In this authentication method/system,
a password is inputted for
execution of a transaction and at the same time the
pressure pattern data
corresponding to the inputted characters are
collated with the pattern data
which are previously registered via a keyboard
consisting of a pressure sensor
such as a piezoelectric element, etc. Thus, it's
possible to prevent the wrong
transaction of a third person who acquired wrong a
password and also to erase
the data by sending a data erasing program to an IC
card from the outside by
radio or the infrared rays.

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The authentication approach and the whole system schematic diagram of the financial transaction of this invention which consist of a financial transaction terminal, an authentication system, a network, and an IC card.
[Drawing 2] The equipment configuration of said financial transaction terminal.
[Drawing 3] The equipment configuration of said authentication system.
[Drawing 4] The equipment configuration of said IC card.
[Drawing 5] It is the processing flow which receives the contract information on IC card data, measures input-statement character data and alphabetic character input-control-pressure data to a dealings demand to a financial transaction terminal, and is transmitted to an authentication system.
[Drawing 6] It is the processing flow carry out retrieval collating in the password and pressure pattern data attest a dealings person based on the dealings demand from said financial transaction terminal 1 and the contract information on a dealings claimant, and the contract information on the dealings claimant which receives the pressure data to an alphabetic character input, and is registered beforehand, and answer a letter in an authentication result (dealings authorization, dealings refusal, unfair-dealings decision) to said financial transaction terminal 1.
[Drawing 7] When the authentication result from said authentication system 2 is received, dealings activation or a dealings refusal message, and re-password input directions are displayed on a dealings claimant and it is judged as an unfair-dealings person, it is the processing flow which transmits the program which eliminates the data which an IC card memorizes.
[Drawing 8] It is a processing flow in the C card which receives and memorizes a data elimination program from said financial transaction terminal 1, and performs data elimination.
[Drawing 9] It is the example which shows the contact condition at the time of the alphabetic character input of the input section of said financial transaction terminal 1, and the dealings claimant of an input keyboard and an input keyboard.
[Drawing 10] It is the example of the contract information with which the dealings claimant which memorizes to said IC card 3 and transmits to a financial institution terminal at a dealings demand makes a contract of a financial institution and dealings.
[Drawing 11] It is the example of the input password of a dealings demand, and the data of input-control-pressure data transmitted to said authentication system 2 from said financial transaction terminal 1.
[Drawing 12] In said authentication system 2, it is the example of a collating agency password and a pressure pattern data table which is collated with the dealings requested data received from said financial transaction terminal 1 and which is registered beforehand.
[Drawing 13] In said authentication system 2, it is the example of the collating resulting table of the dealings requested data received from said financial transaction terminal 1, the collating agency password registered beforehand, and a pressure pattern data table.
[Drawing 14] In said authentication system 2, it is the example of the count count table of an error of the

unfair-dealings decision which counts the count of an input error to the dealings demand from said financial transaction terminal 1 performed repeatedly.
[Drawing 15] It is the example of data of the authentication result which answers a letter from said authentication system 2 to said financial transaction terminal 1.
[Drawing 16] In said IC card 3, it is the example of the dealings data table in which data elimination is carried out by the data elimination program received from said financial transaction terminal.
[Drawing 17] It is the example which sets up the permission data range based on the upper limit and minimum which set up the regression line based on the pressure data of the time series of the data of past dealings in said authentication system 2, and were set as arbitration from the regression line.
[Description of Notations]
1 -- Financial transaction terminal 2 -- Authentication system 3 -- An IC card, 4 -- Network, 11 -- A control section, 12 -- Input section 12113 -- Display, 14 -- The data-processing section, 15 -- Data accumulation section 16 [-- IC card interface,] -- A data test section, 17 -- The transceiver section, 18 111 [21 -- A control section, 22 -- Authentication section,] -- A whole control section, 112 -- The data control section, 113 -- Communications control section 23 -- The data-processing section, 24 -- The pattern data generation section, 25 -- Authentication data accumulation section, 26 -- The transceiver section, 27 -- Alarm section 211 -- A whole control section, 212 -- Data control section, 213 -- Communications control section 214 [-- Storage section / 33 / 311 / -- Communications control section. / -- A whole control section 312 -- The storage control section, 313 / -- The data-processing section 34 -- Transceiver section] -- The data check section, 31 -- A control section, 32

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Customers who contract a financial transaction contract with a financial institution, such as an individual and a corporation, this invention to a financial transaction demand The pressure pattern data to the input keyboard at the time of inputting input-statement characters, such as a password which attests dealings, are used. the dealings demand which led the financial transaction terminal especially -- being related -- an applicable dealings person -- beforehand -- registration -- or The pressure pattern data hysteresis at the time of inputting in the past is accumulated and referred to. It compares with the pressure pattern data to the input keyboard in the case of the dealings demand concerned. A dealings contractor's contract information which refused the dealings demand of the third person who tried to conduct unjust dealings, and was further memorized by the IC card medium which a third person receives unjustly and holds, It is the authentication approach and system in the suitable financial transaction for use in security management. [in the electronic banking which led the over-the-counter transaction of the financial institution which eliminates dealings information, home banking, firm banking, and a transmission line]
[0002]
[Description of the Prior Art] When the electronic banking which led the over-the-counter transaction of a financial institution, home banking, firm banking, and a transmission line performs a financial transaction, connecting row ****** is performing open transmission lines, such as a financial transaction terminal of a financial institution or a customer's financial transaction terminal, a public line, the Internet, and a personal computer, for the individual humanity news, the contract information, and the keyword which attest dealings. as the approach of preventing unfair dealings according [an information system] to spoofing when performing a financial transaction through the financial transaction terminal and network of a financial institution -- an ID number, a password, circuit authentication, electronic signature, and him -- there is authentication etc.
[0003] The conventional approach like the data security method of a publication in a ****** No. 61832 [five to] official report In the system equipped with two or more terminal units and processors, the right information of use which shows available business is beforehand registered in a password for every user. The registered contents were compared with the password entered from the terminal when a user performed business, and the right information of use, and only when it judged with judging whether an operating processing demand is received and receiving, there was a method of performing processing corresponding to an operating processing demand.
[0004] two or more lines which were able to earn the conventional approach on the electrode base like a personal authentication method given in a ****** No. 85276 [seven to] official report -- there was an approach the fingerprint input section which consists of the contact electrode, an electrode sheet, a pressure-sensitive sheet, and a counterelectrode performed personal authentication by regarding the pressurization condition of a finger as a change in resistance, and reading contact resistance.
[0005]

[Problem(s) to be Solved by the Invention] The above-mentioned conventional technique cannot prevent unfair dealings to those who can know the password which attests dealings at the time of a financial transaction. In case he performs a password input for a password, a third person may be able to receive a password by check by looking. Or in order to prevent spoofing, consideration of easy dealings actuation of a dealings person, such as requiring periodical modification of a password and a complicated input procedure of a dealings person, was not carried out, but there was a problem that easy safe and dealings could not be performed. Moreover, in the personal authentication by the body description enquiry of compulsory robbery of a password, a fingerprint, or retina information, there were problems -- the trauma to the body of the dealings person by the third person may be generated. Furthermore, when contract information, dealings information, etc. which are included a non-contact IC card and there are stolen, it cannot prevent the third person who is going to trade unfairly holding those information and using it for others. Moreover, when a data elimination program was carried in the IC card itself, there was a problem that data will be eliminated by malfunction.

[0006] The purpose of this invention associates the input-statement character data at the time of a dealings person's dealings input, and the pressure data to an input keyboard, and is to prevent the thing to which a third person receives and forms a password by collating with the pressure pattern data registered beforehand and in which it trades unfairly more better. Moreover, by check by looking, as for the pressure pattern data to an input keyboard, acquisition cannot obtain a third person unjustly difficultly. Furthermore, when judged with unfair dealings, data elimination by malfunction can protect by transmitting a data elimination program for the contract information and the dealings information which an unfair-dealings person holds to media, such as a noncontact IC card, from the exterior, and making the information which an unfair-dealings person holds by performing a data elimination program by the data-processing section on an IC card eliminate appropriately, and transmitting a data elimination program from the exterior to media, such as an IC card.

[0007]

[Means for Solving the Problem] In order that this invention may attain the above-mentioned purpose, the authentication approach and system in a financial transaction of this invention In case the password which attests dealings is entered, input-statement character data are inputted by the input section. The pressure data produced by the finger part in contact with an input keyboard are measured as an electrical-potential-difference value by the data test section which consists of a piezoelectric device. It is characterized by transmitting the electrical-potential-difference value over the whole input keyboard to an authentication system by the transceiver section, receiving this electrical-potential-difference value data in an authentication system, and having the authentication section which collates the pressure pattern data at the time of dealings, and said pressure pattern data corresponding to the alphabetic character registered beforehand.

[0008] moreover , in order to attain the above-mentioned purpose , the authentication approach and the system of this invention in a financial transaction carry out have the transceiver section which transmit and receive a data elimination program by radio or infrared means of communications , the are recording section which accumulate a data elimination program , and the data processing section perform as the description as an eliminate - contract information [which be accumulate in an IC card] , and dealings information means , when judge as unfair dealings in an IC card and a financial transaction terminal .

[0009] In the financial transaction terminal in which it trades with a financial institution as an operation based on the above-mentioned means By transmitting to media, such as an IC card, when dealings are attested based on two or more information and the program which eliminates the data which an inaccurate dealings person holds is attested with unfair dealings a third person -- him -- it prevents that authentication information comes to hand unjustly, and when unfair dealings by the third person are prevented and it is judged as unfair dealings at the time of a financial transaction, unjust use of the information by the inaccurate third person can be prevented by eliminating the information on an IC card.

[0010]

[Embodiment of the Invention] Hereafter, the example of this invention is explained to a detail based on

a drawing. The block block diagram of the financial transaction terminal whose drawing 1 is the authentication approach and the whole system conceptual diagram in the financial transaction which shows one example of this invention and whose drawing 2 is the important section, the block block diagram with which drawing 3 constitutes an authentication system, and drawing 4 are the block block diagrams of an IC card.

[0011] In drawing 1 , an individual or a company with a financial institution and dealings uses 1. The contract information for the financial transaction which leads the shop front of a financial institution, or a network, Carry out transceiver management of the dealings information etc., and alphabetic data, such as a password entered for dealings authentication of a dealings person, and the pressure data at the time of an alphabetic character input are transmitted to an authentication system. The authentication result from an authentication system is received. And dealings activation or reinput reception of a password, If an authentication system judges it as unfair dealings to the attempt of the input of the multiple times which are not in agreement with the registered input-statement character pattern data and the input-control-pressure pattern data at the time of dealings, a send alarm is carried out to a financial transaction terminal and a financial transaction terminal receives an alarm It is the financial transaction terminal which transmits a data elimination program to the IC card which is judged to be said unfair dealings and is used. 2 is an authentication system which carries out reception management of the data transmitted from the financial transaction terminal, generates pattern data, carries out collating processing based on the received alphabetic data, and pressure data and the data registered beforehand, attests the dealings at the time of a financial transaction, and answers a financial transaction terminal in an authentication result. 3 is data carriers, such as an IC card used in case a dealings claimant transmits and receives a financial transaction terminal and dealings data. 4 is a transmission line including a dedicated line and an open network.

[0012] In drawing 2 , the financial transaction terminal 1 consists of a control section 11, the input section 12, a display 13, the data-processing section 14, the data accumulation section 15, a data test section 16, the transceiver section 17, and an IC card interface 18. Among these, the whole above-mentioned control device 11 consists of a whole control section 111, the data control section 112, and the communications control section 113. In drawing 3 R> 3, the authentication system financial institution terminal 2 consists of a control section 21, the authentication section 22, the data-processing section 23, the pattern data generation section 24, the authentication data accumulation section 25, the transceiver section 26, and an alarm 27. Among these, the above-mentioned control section 21 consists of the whole control section 211, the data control section 212, the communications control section 213, and the data check section 214. In drawing 4 R> 4, IC card 3 consists of a control section 31, the storage section 32, the data-processing section 33, and the transceiver section 34. Among these, a control section 31 consists of a whole control section 311, a memory control unit 312, and the communications control section 313. Drawing 5 is a processing flow which receives the contract information on IC card data, measures input-statement character data and alphabetic character input-control-pressure data to a dealings demand to a financial transaction terminal, and is transmitted to an authentication system.

[0013] Said financial transaction terminal 1 receives the contract information memorized to an IC card given in drawing 1010 with the IC card interface 18 from a dealings claimant to a dealings demand (step 101), and receives the password input which attests dealings by the input section 12 (step 102). At this time, electrical-potential-difference value data are measured from the alphabetic character input control pressure of a dealings person's finger part to an input keyboard and an attached piezoelectric device given in drawing 9 by the data test section 16 (step 103), and the input-statement character data of a publication and input-control-pressure data are transmitted to an authentication system at drawing 11 (step 104). Drawing 6 is the processing flow carry out retrieval collating in the password and pressure pattern data attest a dealings person based on the dealings demand from said financial transaction terminal 1 and the contract information on a dealings claimant, and the contract information on the dealings claimant which receives the pressure data to an alphabetic character input, and is registered beforehand, and answer a letter in an authentication result (dealings authorization, dealings refusal, unfair-dealings decision) to said financial transaction terminal 1.

[0014] Said authentication system 2 receives the input-statement character data and pressure pattern data which are transmitted from the financial transaction terminal 1 in the transceiver section 26 (step 105), and first searches the password with which the publication is beforehand registered into drawing 12 in the authentication data accumulation section 25, and the table of the pressure pattern data generated in the pattern data generation section 24 (step 106). Next, the password, the pressure pattern data and the password of a dealings demand, and pressure pattern data with which this dealings person that searched is registered are collated with drawing 13 on the check table of a publication (step 107). At this time, the check (step 108) of a password and a pressure pattern check (step 109) are performed, and the pressure permission data range to an input keyboard is set up based on the pressure data at the time of the past dealings, and the range check of data is performed (step 110). Furthermore, to the input error of the dealings demand of the same dealings claimant performed repeatedly, the authentication result of dealings refusal is transmitted to said financial transaction terminal 1 of a dealings claimant (step 114). in addition -- and whether it counted with the count count table of an error given [the count of dealings] in drawing 14 (step 112), and the count of an error exceeded the predetermined number of arbitration, and when it checked and (step 113) exceeds, said financial transaction terminal is answered in unfair-dealings decision (step 115). Drawing 7 is a processing flow which transmits the program which eliminates the data which an IC card memorizes, when the authentication result from said authentication system 2 is received, dealings activation or a dealings refusal message, and re-password input directions are displayed on a dealings claimant and it is judged as an unfair-dealings person.

[0015] Said financial transaction terminal 1 receives the authentication result of a publication from an authentication system 2 to drawing 15 (step 116). Confirm whether to be dealings authorization from an authentication result (step 117), if it is dealings authorization, will perform dealings of dealings claimants (step 118), and if it is not dealings authorization Next, from an authentication result, if an unfair-dealings check (step 119) is performed and an authentication result is dealings refusal A dealings refusal message is displayed (step 120), re-password input directions are performed (step 121), and if an authentication result is unfair-dealings decision further, a data elimination program will be transmitted to media, such as an IC card, (step 122). Drawing 8 is a processing flow in the IC card which receives and memorizes a data elimination program from said financial transaction terminal 1, and performs data elimination.

[0016] Said IC card 3 receives the data elimination program from a financial transaction terminal in the transceiver section 34 (step 123), and stores it temporarily in the storage section 32, and elimination of the contract data memorized in the storage section 32 in the data-processing section 33 and dealings data given in drawing 16 is performed (step 124). Moreover, a data elimination program is memorized in an authentication system, and it includes transmitting to a financial transaction terminal and an IC card. the piezoelectric device by which drawing 9 R> 9 is an example which shows the contact condition at the time of the alphabetic character input of the input section of said financial transaction terminal, and the dealings claimant of an input keyboard and an input keyboard, and 121 is installed in the part which contacts in case the finger part on an input keyboard is an alphabetic character input -- last ** Drawing 17 is an example which sets up the permission data range based on the upper limit and minimum which set up the regression line based on the pressure data of the time series of the data of past dealings in said authentication system 2, and were set as arbitration from the regression line.

[0017]

[Effect of the Invention] By according to this invention, carrying out by doubling said authentication approach with a password etc., when the customer who performs financial transactions, such as transfer of fund to a financial institution, close payment, and settlement of accounts, gives a dealings demand to a financial institution It is expectable to be able to prevent unfair dealings, also when a customer's password is acquired unjustly and it is carried out, to eliminate the contract information on the IC card which the third person who tries unfair dealings holds, and dealings information, and to prevent the unauthorized use of this information.

[Translation done.]